7. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. **Tecnologia da informação – Código de prática para a gestão da segurança da informação (NBR ISO/IEC 17799)**. Rio de Janeiro, RJ: 2001.

BRADASCHIA, L. R. **Plano de Continuidade de Negócios**. São Paulo, SP: 2002.

CAMPOS, Stela. **Guarda-costas da informação**. 2003.

CARTWRIGHT, W. **Managing security in a mobile environment. Sans Institute**. 2001.

CHAPMAN, D. B., ZWICKY E. D. **Building Internet Firewalls**. O'Reilly & Associates, 1995.

CHEN, A. **Companies strike back at mobile hacks**. EWeek. 2000.

CERT. **Overview of Attack Trends**. Pittsburgh, PA: 2002.

COBB, S. **The mother of all security standarts?** 2001. Disponível em: <http://www.infosec.spectria.com/articles/ art-bs7799.htm>. Acesso em: 20 dez. 2003.

COLTRO, Renata. **Como estabelecer uma cultura de segurança**. 2000. Disponível em: <http://www.sit.com.br/ SeparataGTI059.htm>. Acesso em: 8 fev. 2003.

COMPTIA. **CompTIA Research: Measuring the Pulse of the IT Industry**. 2002.

CORREIA, André. **Segurança: questão de sobrevivência dos negócios**. 2002. Disponível em: <http://www.infoguerra.com.br/infonews/talk/ 1012557620,12815,.shtml>. Acesso em: 10 mar. 2003.

COUTTO, Fernanda. **Entrevista com Fernando Marinho, CIO da Storm Security**. 2003. Disponível em: <http://www.multivirtual.com.br/ informacao/artigos.php?codigo=72>. Acesso em: 17 jan. 2003.

D'ANDRÉA, E. **Cuide de seus dados**. 2003.

DRI. **Professional Practices for Business Continuity Planners**. 2002.

FAGUNDES, E. **Disaster Recovery Plan**. 2003. Disponível em: <http://www.efagundes.com/Artigos/Disaster_Recovery_Plan.htm>. Acesso em: 21 abr. 2003.

FEDERAL, Governo. **Decreto nº 3.505**. Brasília, DF: Diário Oficial da União, 2000.

___. **Portaria CH/GSI nº 5**. Brasília, DF: Diário Oficial da União, 2001.

___. **Portaria GSI/PR nº 16**. Brasília, DF: Diário Oficial da União, 2001.

___. **Decreto nº 4.553**. Brasília, DF: Diário Oficial da União, 2002.

FERREIRA, G. **Disponibilidade do ambiente: o que fazer**. 2002.

FIGUEIRÊDO, L. S. **Segurança da Tecnologia da Informação**. MG: 2002.

FITES, M., KRATZ P., BREBNER A. **Control and Security of Computer Information Systems**. New York, NY: Computer Science Press, 1989.

GALVÃO, M., POGGI, E. **Avaliação de Riscos em Segurança da Informação com o Security Check-up**. 2002.

GAO. **Federal Information System Controls Audit Manual**. 1999.

___. **Information Security Risk Assessment**. 1999.

GIL, Antônio de Loureiro. **Segurança Empresarial e Patrimonial**. São Paulo: Atlas, 1995.

GOLDANI, Carlos Alberto. **Plano de Continuidade de Negócios**. 2001.

GOLDBERG, Ivan. **Glossary of Information Warfare Terms**. 2000. Disponível em: <http://www.psycom.net/ iwar.2.htm>. Acesso em: 19 fev. 2003.

GONÇALVES, F. **Teletrabalho News – e se, de repente, o inesperado acontecer?** 2003.

GONÇALVES, L. R. O. **Pequeno histórico sobre o surgimento das Normas de Segurança**. 2003. Disponível em: <http://www.modulo.com.br/ index.jsp?page=3&catid=2&objid=344&pagecounter=0&idiom=0>. Acesso em: 25 fev. 2003.

HARGER, V. P. **Planejando a Continuidade dos Negócios**. 2003.

HILES, Andrew. **Business Continuity Management**. 1999. Disponível em: <http://www.davislogic.com/bcm.htm>. Acesso em: 18 jan. 2003.

HIRSCH, J. L. **Telecommuting: security policies and procedures and procedures for the "work-from-anywhere" workforce**. Sans Institute. 2000.

IBM. **Notícias**. 2002. Disponível em: <http://www.ibm.com/ news/br/2002/10/24-10-02.htm>. Acesso em: 15 fev. 2033.

IDC. **A Guide to Business Continuity Planning: Protection and Recovery Services for Your Communications Infrastructure**. 2001.

IDG. **Gartner: 80% dos negócios não têm planos de continuidade**. 2002. Disponível em: <http://idgnow.terra.com.br/idgnow/corporate/ 2002/05/0002>. Acesso em: 23 mar. 2003.

___. **Brasil é líder em TI na América Latina**. 2003. Disponível em: <http://idgnow.terra.com.br/idgnow/business/2003/ 02/0039>. Acesso em: 5 jun. 2003.

___. **Mercado de segurança deve chegar a US$ 45 bi em 2006**. 2003. Disponível em: <http://worldtelecom.idg.com.br/wt/mercado/2003/02/0006>. Acesso em: 8 jul. 2003.

___. **5ª Pesquisa de Comércio Eletrônico no Mercado Brasileiro**. 2003. Disponível em: <http://www.computerworld.com.br/AdPortalV3/ adCmsDocumentoShow.aspx?Documento=24216>. Acesso em: 22 mar. 2003.

___. **Executivos dos EUA não se preocupam com desastres de TI**. 2003. Disponível em: <http://idgnow. terra.com.br/idgnow/business/2003/07/0085>. Acesso em: 27 jan. 2003.

___. **Segurança: ameaças impulsionam investimentos**. 2003. Disponível em: <http://computerworld.terra.com.br/AdPortalV3/adCmsDocumentoShow.aspx?Documento=24980>. Acesso em: 17 fev. 2003.

INFOSEC. **Security Awareness Training**. Texas A&M University, TX: s.d. Disponível em <http:// infosec.tamu.edu/sat/terms.htm>. Acesso em: 16 mar. 2003.

ISO. **Information Security Incident Management (ISO N3017)**. Berlim: 2002.

ITS. **Federal Standard 1037C**. Colorado: 1996. Disponível em: <http://www.its.bldrdoc.gov/fs-1037/dir-019/_2726.htm>. Acesso em: 13 jun. 2003.

KING, E. **Have Business Learned the Lessons of September 11?** 2002. Disponível em: <http://www.winnetmag.com/WindowsStorage/Article/ ArticleID/26563/WindowsStorage_26563.htm>. Acesso em: 29 mai. 2003.

KPMG. **Planejamento da Continuidade dos Negócios**. 2002.

LOPES, F. A. P. **A Proteção do Conhecimento Sensível em Empresas do Rio Grande do Sul**. São Leopoldo, RS: 2000.

MACHADO, M. P. **Análise e Estudo de Segurança de Corporações Utilizando Firewalls**. 2002.

MCDANIEL, George. **IBM Dictionary of Computing**. New York, NY: McGrow-Hill, 1994.

MCLEAN, J. **Security Models**. 1994.

MCT. **Decreto nº 4.553**. Brasília, DF: Diário Oficial da União, 2002. Disponível em: <http://www.mct.gov.br/ legis/decretos/4553_2002.htm>. Acesso em: 14 mai. 2003.

MIT. **Business Continuity Plan**. 2002.

MÓDULO. **7ª Pesquisa Nacional de Segurança da Informação**. 2001.

___. **8ª Pesquisa Nacional de Segurança da Informação**. 2002.

___. **PCN não é prioridade de pequenas e médias empresas européias**. 2003. Disponível em: <http://www. modulo.com.br/index.jsp?page=3&catid=7 &objid=1670&pagecounter=0&idiom=0>. Acesso em: 19 abr. 2003.

MOORE, Pat. Business Continuity Planning. **Facility Management Journal**, 2000.

Morse, Janice M. **Critical Issues in Qualitative Research Methods**. London: SAGE, 1994.

NETO, N. N. **Criptografia em Comunicação de Dados**. São Paulo, SP: 2002.

NEVERFAIL GROUP. **Guide to Disaster Recovery Solutions**. 2002

NILLES, J. M. **What does telework really do to us?** Word Transport Policy & Practice. 1996.

NIST. **Generally Accepted Principles and Practices for Securing Information Technology Systems (sp800-14)**. 1996.

OECD. **Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**. França: 2002.

PEREIRA, Cristiane. **Implementação de Políticas e Procedimentos de Segurança em Ambiente Internet**. Brasília, DF: 2000.

PINTO, Elaine. **Segurança da informação em documentos oficiais**. 2003. Disponível em: <http://www.modulo.com.br/index.jsp?page=3&catid=2& objid=318&pagecounter=0&idiom=0>. Acesso em: 21 fev. 2003.

PORTER, Michael. **Vantagem Competitiva**. RJ: Campus, 1992.

PRICEWATERHOUSECOOPERS. **Empresas aumentam investimentos em segurança**. 2003. Disponível em: <http://www.csoonline.com.br/AdPortalV3/adCmsDocumentoShow.aspx?documento=25228&Area=1>. Acesso em: 11 jun. 2003.

PRITCHARD, Kate. **Banking on Technology**. 2003. Disponível em: <http://www.emc.com/continuity/related/0302_ fastcompanies.jsp>. Acesso em: 13 jan. 2003.

PURCELL, J. **Securing information on laptops computers**. Sans Institute. 2000.

REID, F. **Securing the mobile businessman**. Sans Institute. 2000.

ROCHA, L. F. **Entrevista com Bruce Schneier**. 2002. Disponível em: <http://www.modulo.com.br/index.jsp?page=3&catid=6&objid=34&pagecounter=0&idiom=0>. Acesso em: 17 abr. 2003.

___. **Aumenta o número de empresas certificadas BS 7799 pelo mundo**. 2003. Disponível em: <http://www. modulo.com.br/index.jsp?page=3&catid=7&objid=1732&pagecounter=0&idiom=0>. Acesso em: 18 mai. 2003.

SANS. **Introduction to Business Continuity Plan**. Sans Institute. 2002.

SCHNEIER, B. **Applied Cryptography**. NY: John Wiley & Sons, 1996.

SÊMOLA, Marcos. **Entrevista de Marcos Sêmola**. RJ: Informática ETC, 2003.

SOUZA MACHADO, C. **MSIST – Modelo de Segurança para Sistemas de Teletrabalho**. Enanpad. 2002.

SYMANTEC. **Pesquisa de Segurança de Sistemas e Informações**. 2002.

TZU, Sun. **A Arte da Guerra**. Porto Alegre, RS: L&PM Editores, 2001.

VERGARA, S. C., **Projetos e Relatórios de Pesquisa em Administração.** 3ª ed. São Paulo, SP: ATLAS Editora, 2000.

Weber, Robert Philip. **Basic Content Analysis**. Newbury Park, CA: Sage Publications, 1990.

WEBOPEDIA. **Security**. 2002. Disponível em: <http://www.webopedia.com/term/s/security.htm>. Acesso em: 24 jan. 2003.

WHATIS.COM. **Business Continuance**. 2002. Disponível em: <http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci801381,00.htm>. Acesso em: 15 mar. 2003.

8. ANEXOS

8.1. Organizações atuantes em SI

Institutos, organizações e empresas atuantes na área de segurança da informação

3COM

Empresa especializada em tecnologias de rede de dados com atuação também na área de segurança.

http://www.3com.com

ABIN – Agência Brasileira de Informação

A ABIN desenvolve o Programa Nacional de Proteção ao Conhecimento (PNPC) que procura sensibilizar segmentos da sociedade brasileira sobre as ameaças ao desenvolvimento e à segurança nacionais, representadas pelas ações de espionagem em alvos econômicos, industriais e científico-tecnológicos.

http://www.abin.gov.br/abin/index.jsp

ASIS

Organização dedicada em aumentar a eficiência e a produtividade das práticas de segurança.

http://www.asisonline.org/

AT&T

Empresa que oferece serviços de recuperação de desastres na área de telecomunicações.

http://www.att.com/presskit/business_continuity/

http://www.att.com/ndr/

AusCERT

Centro de pesquisas em segurança da Austrália.

http://www.auscert.org.au/

Business Continuity Institute

Instituto criado em 1994 para prover suporte aos profissionais que trabalham com continuidade de negócios.

http://www.thebci.org/

CAIS - Centro de Atendimento a Incidentes de Segurança

O CAIS atua na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes.

http://www.rnp.br/cais/

CIS – The Center of Internet Security

Organização sem fins lucrativos que visa a auxiliar empresas a reduzir os riscos relacionados à segurança da informação.

http://www.cisecurity.org/

CERT – Computer Emergency Response Team

Centro de pesquisas em segurança da Universidade de Carnegie Mellon.

http://www.cert.org/

CESG - Communications-Electronics Security Group

Órgão oficial do governo britânico para assuntos de segurança da informação.

http://www.cesg.gov.uk/

CSI – Computer Security Institute

Instituto que organiza conferências, seminários e disponibiliza publicações sobre SI.

http://www.gosci.com/

CSRC – Computer Security Resource Center

Divisão do NIST (National Institute of Standards and Technology) responsável por pesquisar, estudar, alertar e desenvolver padrões na área de segurança da informação.

http://csrc.nist.gov/

DRI – Disaster Recovery Institute

Instituto com reconhecimento internacional por sua atuação na área de segurança da informação. Seu guia de práticas para PCN é observado por diversas organizações.

http://www.drii.org

DRJ – Disaster Recovery Journal

Revista dedicada ao tema continuidade dos negócios desde 1987.

http://www.drj.com

Equipe de Segurança em Sistemas e Redes

Equipe responsável pela segurança da informação da UNICAMP.

http://www.security.unicamp.br/

GAMMA

Empresa que fornece serviços de consultoria na área de SI.

http://www.gammassl.co.uk/

GTS - UNESP

Site do Grupo de Trabalho em Segurança da Universidade Estadual Paulista

http://www.unesp.br/gts/

IEC - International Engineering Consortium

Organização que atua na promoção do desenvolvimento de novas tecnologias na indústria da informação.

http://www.iec.org/

IEEE Security & Privacy

Site que disponibiliza artigos, casos de estudo e tutoriais sobre o tema segurança da informação.

http://computer.org/security/

IETF – Internet Engineering Task Force

Organismo internacional que congrega profissionais e pesquisadores atuantes na Internet.

http://www.ietf.org/

Information Security Forum

Associação internacional que desenvolve pesquisas sobre SI.

http://www.securityforum.org/

Information Security Magazine

Revista eletrônica especializada em notícias sobre o mundo da segurança.

http://www.infosecuritymag.com/

INFOSEC - Information Security Office

Departamento de segurança da informação da Texas A&M University.

http://infosec.tamu.edu/

ISACA - Information Systems Audit and Control Association & Foundation

Organização que dissemina práticas de controle e auditoria para a área de TI. Desenvolveu o padrão *COBIT - Governance, Control and Audit for Information and Related Technology*

http://www.isaca.org/

ISO – International Organization for Standardization

Organização internacional responsável por criar padrões em diversas áreas do conhecimento.

http://www.iso.org/

ISSA – Information Systems Security Association
Organização sem fins lucrativos que atua na área de SI.
http://www.issa.org/

IT Security
Site especializado em SI.
http://www.itsecurity.com/

LARC
Laboratório de Arquitetura e Redes de Computadores da USP.
http://www.redes.usp.br/

LSE Computer Security Research Centre
Centro britânico que estuda segurança da informação.
http://csrc.lse.ac.uk/

MIT Information Security Office
Departamento de segurança da informação do MIT - Massachusetts Institute of Technology.
http://web.mit.edu/security/www/

Módulo Security
Empresa especializada no segmento de segurança da informação.
http://www.modulo.com.br

NBSO
Grupo de Resposta a Incidentes para a Internet Brasileira, mantido pelo Comitê Gestor da Internet no Brasil.
http://www.nbso.nic.br/

OECD

Organização para Cooperação e Desenvolvimento Econômico.
http://www.oecd.org/EN/home/0,,EN-home-43-nodirectorate-no-no-no-13,00.html

Organisation for Internet Safety

Organização que congrega vendedores de software e pesquisadores de vulnerabilidades, a fim de estabelecer práticas comuns para lidar com descobertas de falhas em sistemas.
http://www.oisafety.org/

SANS' Information Security Reading Room

Organização que oferece farta documentação sobre diversos assuntos relativos à segurança da informação.
http://www.sans.org/rr/

Security Management Online

Publicação voltada para o segmento de SI com mais 33000 membros em todo o mundo.
http://www.securitymanagement.com/

Security Forum

Fórum dedicado à segurança da informação, mantido pelo The Open Group.
http://www.opengroup.org/security/more.htm

Symantec

Empresa especializada no segmento de segurança da informação.
http://www.symantec.com/

TI Brasil Intelligence

Empresa que promove seminários sobre segurança dos dados corporativos.
http://www.ti-intelligence.com.br/

8.2. Classificação das informações

A classificação das informações é essencial para se conceber uma melhor proteção aos dados confidenciais das organizações. Com base na classificação é possível estabelecer critérios de acesso para garantir que somente pessoas autorizadas tenham conhecimento das informações contidas nos documentos presentes nos mais variados tipos de dispositivo, como papel, fitas, disquetes, bancos de dados e outros (Pinto, 2003).

É possível ilustrar a importância de existir diferentes níveis de acesso com o seguinte exemplo (Machado, 2002): alguns fabricantes de carros projetam as trancas de forma que uma chave abre a porta e a ignição, mas uma outra diferente abre o porta-malas e porta-luvas. Assim, é possível entregar a um guardador de carros – que deve ter somente o privilégio de abrir a porta e dirigir o carro até a vaga – somente a primeira chave, mantendo os outros compartimentos inacessíveis.

Os funcionários de uma organização precisam de determinado nível de acesso para desempenharem suas respectivas funções, porém a falta de adequação do critério de acesso às reais necessidades de cada um é um sério problema de segurança que deve ser revisto com urgência.

Segundo pesquisa do The Data Warehousing Institute (D'Andréa, 2003), a falta da qualidade das informações, que inclui problemas de disponibilidade e integridade, gera custos de 611 bilhões dólares por ano para as empresas americanas.

O decreto nº 4.553 (MCT, 2002) do governo brasileiro, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado trata também sobre a classificação segundo o grau de sigilo. Alguns trechos retirados do decreto:

> *Art. 5º Os dados ou informações sigilosos serão classificados em ultra-secretos, secretos, confidenciais e reservados, em razão do seu teor ou dos elementos intrínsecos.*

> *§ 1º São passíveis de classificação como ultra-secretos, dentre outros, dados ou informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.*
>
> *§ 2º São passíveis de classificação como secretos, dentre outros, dados ou informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não-autorizado possa acarretar dano grave à segurança da sociedade e do Estado.*
>
> *§ 3º São passíveis de classificação como confidenciais dados ou informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.*
>
> *§ 4º São passíveis de classificação como reservados dados ou informações cuja revelação não autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.*

Segundo ainda Pinto, assim como o decreto prevê a classificação das informações segundo o grau de sigilo no âmbito da Administração Pública Federal, as empresas por meio de sua política corporativa de segurança da informação também devem estabelecer critérios para classificar as suas informações, considerando os princípios de confidencialidade, integridade e disponibilidade.

Ferreira (2002) sugere a seguinte classificação das informações:

Classificação	Descrição
Vitais	▪ Impacto vital nos negócios ▪ Continuidade dos serviços é fundamental
Críticas	▪ Campanhas, compras, distribuição, esquemas de produção, controle financeiro ▪ Tratar após emergência
Normais	▪ Auditoria, RH, marketing, planos de produção, planos de longo prazo, qualidade, treinamento, desenvolvimento ▪ Suspender operação e tratar quando possível

Tabela 8: Classificação das informações (Ferreira, 2002)

Para fechar este anexo, citamos Machado (2002) que diz que a abordagem de estabelecer privilégios é um importante princípio para limitar a exposição a ataques e minimizar os possíveis danos causados pelos mesmos. Ou seja, toda empresa deve classificar suas informações e prover a segurança adequada a elas.

8.3. Tecnologias de SI

Aqui estão descritas algumas tecnologias utilizadas em segurança da informação. Não é a intenção esgotar o assunto, mas mostrar o que existe de importante na área.

Assinatura digital

Assinatura digital é um código que é incluído na mensagem ou no texto, que identifica o remetente da mensagem.

Certificado digital

Os certificados digitais são arquivos de computador emitidos por entidades certificadoras ou CAs, e tem por objetivo garantir que o emissor de uma mensagem ou documento, é realmente quem ele diz ser.

Criptografia

Criptografia vem do grego kryptós = escondido, oculto + grápho = grafia, escrita. É a arte ou a ciência de escrever em cifra ou em código.

Criptografia é um conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinatário a decifre e compreenda.

Criptografia assimétrica

A Criptografia Assimétrica, também conhecida como de chave pública, utiliza duas chaves, uma para cifrar o texto ou mensagem, e outra para decifrar.

Criptografia simétrica

A Criptografia Simétrica ou de chave secreta, foi o primeiro tipo de criptografia criado. Funciona transformando um texto em uma mensagem cifrada, através da definição de uma chave secreta, que será utilizada posteriormente para descriptografar a mensagem, tornando novamente um texto simples.

Firewall

Firewalls são barreiras interpostas entre a rede privada da organização e a rede externa. O firewall analisa o tráfego entre a rede interna e a rede externa em tempo real, permitindo ou bloqueando o tráfego de acordo com as regras definidas previamente.

IDS - intrusion detection system

O sistema de detecção de intrusos é uma ferramenta utilizada para detectar e alertar sobre ataques e tentativas de acessos indevidos na rede corporativa.

PKI - public key infrastructure

A PKI refere-se a um processo que utiliza chaves públicas e Certificados Digitais para garantir a segurança do sistema e confirmar a identidade de seus usuários.

VPN – virtual private network

VPN é uma rede privada construída dentro da infra-estrutura de uma rede pública, como a Internet, utilizando recursos de criptografia para garantir a integridade, a confidencialidade e a autenticidade dos dados trafegados.

8.4. Questionários

Questionário original

Questionário de Pesquisa sobre Plano de Continuidade de Negócios

Objetivo: este questionário tem como objetivo colher subsídios para retratar o atual estágio de utilização do plano de continuidade de negócios (PCN) nas empresas operando no Brasil.

Quem deve preencher: o profissional de mais alto cargo na área de TI que esteja familiarizado com as práticas de segurança da informação de sua empresa.

O que é desejado ao final: que as respostas ao questionário identifiquem a observância de um plano de continuidade de negócios em diversas empresas operando no Brasil e reportem dificuldades em sua utilização, de modo a servir de alerta para um problema crucial. Enfatizamos que isso não é um teste, onde deveriam ser dadas as "respostas certas", mas sim um instrumento de coleta de dados.

Ressaltamos que os dados fornecidos serão considerados confidenciais, com finalidade estritamente acadêmica, e utilizados apenas para fins desta pesquisa. Assim, não serão, sob qualquer hipótese, repassados a outras pessoas ou instituições, ou utilizados para outros fins. Caso os resultados consolidados da pesquisa sejam divulgados posteriormente, isso será feito sem apontar as respostas específicas de qualquer respondente.

O questionário é dividido em quatro partes: identificação da empresa, identificação do respondente, perguntas fechadas e perguntas abertas. O tempo médio de preenchimento das 25 perguntas é de 20 a 30 minutos.

Instruções para preenchimento:
1) Para responder às questões, basta assinalar no espaço adjacente às opções dadas.
2) Se for o caso, múltiplas opções podem ser assinaladas.
3) Se por alguma razão (confidencialidade, informação incompleta ou quaisquer outras) uma questão não puder ser respondida, ignore-a. Apenas solicitamos que não deixe de responder às demais, pois **toda a informação fornecida será essencial para o prosseguimento desta investigação**.
4) Quaisquer informações adicionais podem ser enviadas em folhas avulsas anexas ao questionário.
5) Atenção! Algumas questões contêm instruções especiais de preenchimento.

Desde já, agradecemos seu tempo e sua colaboração.

Parte 1 - Identificação da Empresa

Empresa:

Divisão:

Faturamento anual no Brasil: R$

Número de funcionários:

Parte 2 - Identificação do Respondente

Cargo:

Nome:

1. Nível gerencial

( )Diretor	( )Gerente	( )Coordenador	( )Analista

2. Deseja receber os dados consolidados desta pesquisa?

( )Sim	( )Não

Caso positivo, digite seu e-mail:

Parte 3 – Perguntas Fechadas

3. A empresa possui um plano de continuidade de negócios?

( )Sim	( )Não

Caso negativo, indique os motivos da não adoção de um PCN:

4. A empresa já realizou alguma análise de risco de suas atividades e recursos?

( )Sim	( )Não	( )Não sei

5. Caso positivo, quando foi realizada a última análise de risco?

( )Há menos de 6 meses	( )De 6 meses a 1 ano	( )Há mais de 1 ano

6. A empresa já realizou alguma análise de impacto em seu negócio?

( )Sim	( )Não	( )Não sei

7. Caso positivo, quando foi realizada a última análise de impacto?

( )Há menos de 6 meses	( )De 6 meses a 1 ano	( )Há mais de um ano

8. Qual é a tendência de variação do orçamento da empresa reservado para plano de continuidade de negócios?

( )Aumentar	( )Manter	( )Diminuir

9. Qual é a tendência de variação do orçamento da empresa reservado para segurança da informação?

( )Aumentar	( )Manter	( )Diminuir

10. Qual é a freqüência anual de revisão do PCN?

( )0 ou menor que 1	( )1	( ) 2 ou mais

11. Qual é a freqüência anual de simulação dos procedimentos contidos no PCN?

( )0 ou menor que 1	( )1	( ) 2 ou mais

12. Abrangência das simulações dos procedimentos (Marque todas as opções que participam das simulações):

( ) Equipe de TI
( ) Todos os funcionários
( ) Fornecedores
( ) Clientes
( ) Serviços públicos (Ex: bombeiro, polícia, água, luz)

13. Qual é a freqüência anual de treinamento em segurança da informação para a equipe de TI?

( )0 ou menor que 1	( )1	( ) 2 ou mais

14. Qual é a freqüência anual de treinamento em segurança da informação para todos os funcionários da empresa?

( )0 ou menor que 1	( )1	( ) 2 ou mais

15. Qual é a freqüência anual de treinamento em continuidade de negócios para a equipe de TI?

( )0 ou menor que 1	( )1	( ) 2 ou mais

16. Qual é a freqüência anual de treinamento em continuidade de negócios para todos os funcionários?

( )0 ou menor que 1	( )1	( ) 2 ou mais

Para as próximas perguntas, assinale a opção que melhor avalia a afirmação em destaque. Considere a seguinte legenda:

DC	Discordo Totalmente
D	Discordo
NDNC	Nem Concordo Nem Discordo
C	Concordo
CC	Concordo Totalmente

17. Segurança da informação é um tema considerado importante por toda diretoria da empresa

( )DC	( )D	( )NDNC	( )C	( )CC

18. Plano de continuidade de negócios é um tema considerado importante por toda diretoria da empresa

( )DC	( )D	( )NDNC	( )C	( )CC

19. A equipe de TI da empresa está bem preparada para agir em casos de incidentes que interrompam suas atividades

( )DC	( )D	( )NDNC	( )C	( )CC

20. Os funcionários da empresa estão bem preparados para agir em casos de incidentes que interrompam suas atividades

( )DC	( )D	( )NDNC	( )C	( )CC

Parte 4 – Perguntas Abertas

21. Percentual do orçamento da empresa reservado para segurança da informação: %

22. Percentual do orçamento da empresa reservado para PCN: %

23. Cite os problemas enfrentados na utilização do PCN e descreva como foram superados

24. Na sua opinião, que medidas a empresa deve tomar para fortalecer a área de segurança da informação?

25. Na sua opinião, que medidas a empresa deve tomar para estar mais bem preparada para enfrentar eventos que paralisem suas atividades?

Muito obrigado!

Questionário aplicado na pesquisa

Questionário de Pesquisa sobre Plano de Continuidade de Negócios

Objetivo: este questionário tem como objetivo colher subsídios para retratar o atual estágio de utilização do plano de continuidade de negócios (PCN) nas empresas operando no Brasil.

Quem deve preencher: o profissional de mais alto cargo na área de TI que esteja familiarizado com as práticas de segurança da informação de sua empresa.

O que é desejado ao final: que as respostas ao questionário identifiquem a observância de um plano de continuidade de negócios em diversas empresas operando no Brasil e reportem dificuldades em sua utilização, de modo a servir de alerta para um problema crucial. Enfatizamos que isso não é um teste, onde deveriam ser dadas as "respostas certas", mas sim um instrumento de coleta de dados.

Ressaltamos que os dados fornecidos serão considerados confidenciais, com finalidade estritamente acadêmica, e utilizados apenas para fins desta pesquisa. Assim, não serão, sob qualquer hipótese, repassados a outras pessoas ou instituições, ou utilizados para outros fins. Caso os resultados consolidados da pesquisa sejam divulgados posteriormente, isso será feito sem apontar as respostas específicas de qualquer respondente.

O questionário é dividido em três partes: identificação da empresa, identificação do respondente e perguntas fechadas. O tempo médio de preenchimento das 21 perguntas é de 15 a 20 minutos.

Instruções para preenchimento:
1) Para responder às questões, basta assinalar no espaço adjacente às opções dadas.
2) Se for o caso, múltiplas opções podem ser assinaladas.
3) Se por alguma razão (confidencialidade, informação incompleta ou quaisquer outras) uma questão não puder ser respondida, ignore-a. Apenas solicitamos que não deixe de responder às demais, pois **toda a informação fornecida será essencial para o prosseguimento desta investigação**.
4) Quaisquer informações adicionais podem ser enviadas em folhas avulsas anexas ao questionário.
5) Atenção! Algumas questões contêm instruções especiais de preenchimento.

Desde já, agradecemos seu tempo e sua colaboração.

Parte 1 - Identificação da Empresa

Empresa:

Divisão:

Faturamento anual no Brasil: R$

Número de funcionários:

Parte 2 - Identificação do Respondente

Cargo:

Nome:

1. Nível gerencial

( )Diretor	( )Gerente	( )Coordenador	( )Analista

2. Deseja receber os dados consolidados desta pesquisa?

( )Sim	( )Não

Caso positivo, digite seu e-mail:

Parte 3 – Perguntas Fechadas

3. A empresa possui um plano de continuidade de negócios?

( )Sim	( )Não

Caso negativo, indique os motivos da não adoção de um PCN:

4. A empresa já realizou alguma análise de risco de suas atividades e recursos?

( )Sim	( )Não	( )Não sei

5. Caso positivo, quando foi realizada a última análise de risco?

( )Há menos de 6 meses	( )De 6 meses a 1 ano	( )Há mais de 1 ano

6. A empresa já realizou alguma análise de impacto em seu negócio?

( )Sim	( )Não	( )Não sei

7. Caso positivo, quando foi realizada a última análise de impacto?

( )Há menos de 6 meses	( )De 6 meses a 1 ano	( )Há mais de um ano

8. Qual é a tendência de variação do orçamento da empresa reservado para segurança da informação?

( )Aumentar	( )Manter	( )Diminuir

9. Qual é a tendência de variação do orçamento da empresa reservado para PCN?

( )Aumentar	( )Manter	( )Diminuir

10. Qual é a freqüência anual de revisão do PCN?

( )0 ou menor que 1	( )1	( ) 2 ou mais

11. Qual é a freqüência anual de simulação dos procedimentos contidos no PCN?

( )0 ou menor que 1	( )1	( ) 2 ou mais

12. Abrangência das simulações dos procedimentos (Marque todas as opções que participam das simulações):

( ) Equipe de TI
( ) Todos os funcionários
( ) Fornecedores
( ) Clientes
( ) Serviços públicos (Ex: bombeiro, polícia, água, luz)

13. Qual é a freqüência anual de treinamento em segurança da informação para a equipe de TI?

( )0 ou menor que 1	( )1	( ) 2 ou mais

14. Qual é a freqüência anual de treinamento em segurança da informação para todos os funcionários da empresa?

( )0 ou menor que 1	( )1	( ) 2 ou mais

15. Qual é a freqüência anual de treinamento em continuidade de negócios para a equipe de TI?

( )0 ou menor que 1	( )1	( ) 2 ou mais

16. Qual é a freqüência anual de treinamento em continuidade de negócios para todos os funcionários?

( )0 ou menor que 1	( )1	( ) 2 ou mais

Para as próximas perguntas, assinale a opção que melhor avalia a afirmação em destaque. Considere a seguinte legenda:

DC	Discordo Totalmente
D	Discordo
NDNC	Nem Concordo Nem Discordo
C	Concordo
CC	Concordo Totalmente

17. Segurança da informação é um tema considerado importante por toda diretoria da empresa

( )DC	( )D	( )NDNC	( )C	( )CC

18. Plano de continuidade de negócios é um tema considerado importante por toda diretoria da empresa

( )DC	( )D	( )NDNC	( )C	( )CC

19. A equipe de TI da empresa está bem preparada para agir em casos de incidentes que interrompam suas atividades

( )DC	( )D	( )NDNC	( )C	( )CC

20. Os funcionários da empresa estão bem preparados para agir em casos de incidentes que interrompam suas atividades

( )DC	( )D	( )NDNC	( )C	( )CC

21. Percentual do orçamento da empresa reservado para segurança da informação

( ) menor que 1%	( ) de 1 a 2%	( ) maior que 2%